

Implantação do Zabbix para monitoramento de infraestrutura

Raphael Celuppi

Curso de Especialização em Redes e Segurança de Sistemas

Pontifícia Universidade Católica do Paraná

Curitiba, Setembro 2009

Sumário

1. Introdução.....	3
2. Descrição do Contexto	3
2.1. Motivação do Projeto	3
2.2. Escolha da Ferramenta	3
2.3. Objetivos	6
2.4. Objetivos Específicos.....	7
3. Descrição do Projeto.....	8
3.1. Diagrama de Blocos.....	8
3.2. Descrição do Diagrama de Blocos	9
4. Procedimentos de Teste e Avaliação.....	15
5. Conclusão.....	20

1. Introdução

Esse artigo tem como objetivo descrever de maneira clara e objetiva a implantação do sistema Zabbix, uma ferramenta de monitoramento de infraestrutura de código aberto com suporte a monitorar uma infinidade de aplicações, servidores e equipamentos de rede. Foi escolhido o Zabbix como ferramenta, pois foi a que apresentou uma solução mais completa para o monitoramento de um ambiente bastante heterogêneo, com suporte a monitorar tanto servidores por agentes próprios e por SNMP v1,v2 e v3, também utilizado para monitorar dispositivos de rede, por sua rápida curva de aprendizagem, gerenciamento centralizado e armazenamento em banco de dados.

2. Descrição do Contexto

2.1. Motivação do Projeto

Precisaríamos em nossa estrutura de uma ferramenta capaz de monitorar diversos hosts e equipamentos diferentes como Windows, Linux, BSD's, Unix e equipamentos de redes utilizando o protocolo SNMP e algumas aplicações como WEB, Oracle entre outros, essa ferramenta teria que armazenar essas informações por um período programado, possuir uma interface web simples de ser gerenciados com controles de acesso, logs de auditoria para garantir a confiabilidade das informações, níveis de alertas com sistema de notificação personalizável.

2.2. Escolha da Ferramenta

O Zabbix [1] foi comparado a algumas ferramentas open source de monitoramento de infraestrutura como o Nagios [2] e o Cacti [3], cujo quais são excelentes ferramentas mas que não possui uma suíte completa de ferramentas como Zabbix, que possui tanto uma interface de monitoramento e alerta em tempo real excelente como o Nagios e também possui histórico de informações e gráficos iguais ao do CACTI nos trazendo assim o melhor das duas ferramentas mais utilizadas atualmente em uma.

Segue abaixo as funcionalidades de cada ferramenta:

Nagios:

- Monitoramento de aplicação, serviços, sistemas operacionais e componentes de infraestrutura.
- API para desenvolvimento de sistemas customizados.
- Cliente proprietário

- Suporte ao protocolo SNMP.
- Visão centralizada de todos os sistemas monitorados.
- Informações detalhadas dos componentes monitorados na interface WEB.
- Rápida detecção de problemas na infraestrutura.
- Alertas via e-mail e SMS.
- Alertas customizáveis, para o envio diretamente a pessoa responsável.
- Base de conhecimento para problemas com soluções conhecidas.
- Configurações de eventos para ações pré-configuradas, como reiniciar o serviço com problema.
- Planejamento de infraestrutura para o acompanhamento do envelhecimento do parque tecnológico.
- Paradas programadas, para o sistema não enviar alertas nesses períodos.
- Relatórios para o acompanhamento dos SLA's.
- Históricos de envio de alertas e notificações.
- Suporte a plugins de terceiros.
- Multiusuário web com níveis de acessos.

Cacti:

- Numero ilimitado de gráficos por host.
- Envio de alertas via e-mail e script personalizado.
- Armazenamento configurável de históricos.
- Rápido resequenciamento dos itens gráficos.
- Suporte completo ao RRDTOOL.
- Suporte ao protocolo SNMP.
- Modelos gráficos pré-configurados.
- Gerenciamento totalmente web.

- Multiusuário web com níveis de acessos.

Zabbix:

- Gerenciamento centralizado
- Acesso centralizado as informações
- Numero ilimitado de proxies.
- Monitoramento em tempo real.
- Monitoramento de alertas para disponibilidade, integridade, entre outros.
- Alertas via e-mail, SMS, mensagem instantânea e via script configurado.
- Log de auditoria.
- Visualização via abas web e mapas.
- Execução de comandos remotos.
- Suporte a serviços de TI hierárquicos.
- Relatórios em tempo real de SLA's.
- Facilidade de integração com sistemas de terceiros.
- Modelos pré-configurados de hosts.
- Facilidade de compartilhamento de modelos.
- Sistema de auto busca de dispositivos a serem monitorados.
- Monitoramento de páginas WEB.
- Suporte a qualquer plataforma.
- Suporte ao protocolo SNMP.
- Agente próprio de alta performance.
- Rápida curva de aprendizagem.
- Multiusuário web com níveis de acessos flexíveis.

2.3. Objetivos

Com a implantação da ferramenta Zabbix em nosso ambiente, temos como foco atingir os objetivos:

- O monitoramento da infraestrutura.
- Armazenamento de histórico do status do sistema para possíveis análise em caso de problemas que ocorram no período em que a empresa não possua um técnico disponível para atender o incidente.
- Relatórios para acompanhamento de disponibilidade do ambiente.
- Relatórios gerenciar para acompanhamento do SLA de aplicações vitais.

Todos esses dados devem ser monitorados e o sistema deve enviar alertas em faixas diferentes de prioridade, cujo qual foi definido como as prioridades padrões do Zabbix que são, sendo a primeira menos prioritária e a ultima mais prioritária:

- Não classificada
- Informação
- Advertência
- Médio
- Alto
- Desastre

Esses níveis serão utilizados para definir cada tipo de incidente que ocorra na infraestrutura, esse incidente poderá acionar um ou mais gatilhos que executara uma ação pré-configurada, que pode variar apenas de enviar um e-mail como executar um comando remoto.

Como objetivo geral da implantação dessa ferramenta, queremos estabelecer altos níveis de qualidade do serviço oferecidos a clientes e colaboradores, definindo SLA's e oferecer relatórios confiáveis que comprovem a disponibilidade e confiabilidade de nossa infraestrutura.

2.4. Objetivos Específicos

Com a implantação da ferramenta de monitoramento, temos o objetivo de garantir o cumprimento de SLA's e relatórios específicos para medição de performance de rede e de aplicações, se fazendo necessário relatórios com os seguintes itens:

- Utilização de rede do host por interface de rede, para monitoramento de performance de rede.
- Utilização de disco rígido por host, para projeção de utilização de disco rígido.
- Utilização de CPU, para diagnóstico de performance.
- Utilização de Memória, para diagnóstico de performance.
- I/O de disco rígido, para diagnóstico de performance.
- Delay de ping do host, para diagnóstico de performance e cumprimento de SLA.
- Monitoramento de acesso a aplicações WEB com tempo de carregamento de página, com suporte a configurações de cenários de acesso, para monitoramento de SLA's de aplicação.
- Monitoramento de hash de arquivos, para detectar alterações não autorizadas de arquivos.
- Acesso a histórico de alertas emitidos, para fins históricos.
- Relatório de acionamento dos gatilhos (*triggers*), para fins históricos.
- Relatório de disponibilidade dos hosts, por período configurável, para monitoramento de SLA.
- Gráficos dos dados monitorados por período configurável, para relatórios gerenciais.
- Monitoramento do tempo para se estabelecer uma conexão TCP, para cumprimento de SLA.
- Histórico de todas as ações executadas pelo sistema de monitoramento e pelos usuários nele cadastrado, para fins de auditoria.

3. Descrição do Projeto

3.1. Diagrama de Blocos

A implantação inicial de o sistema ira seguir o seguinte diagrama [Figura 1]:

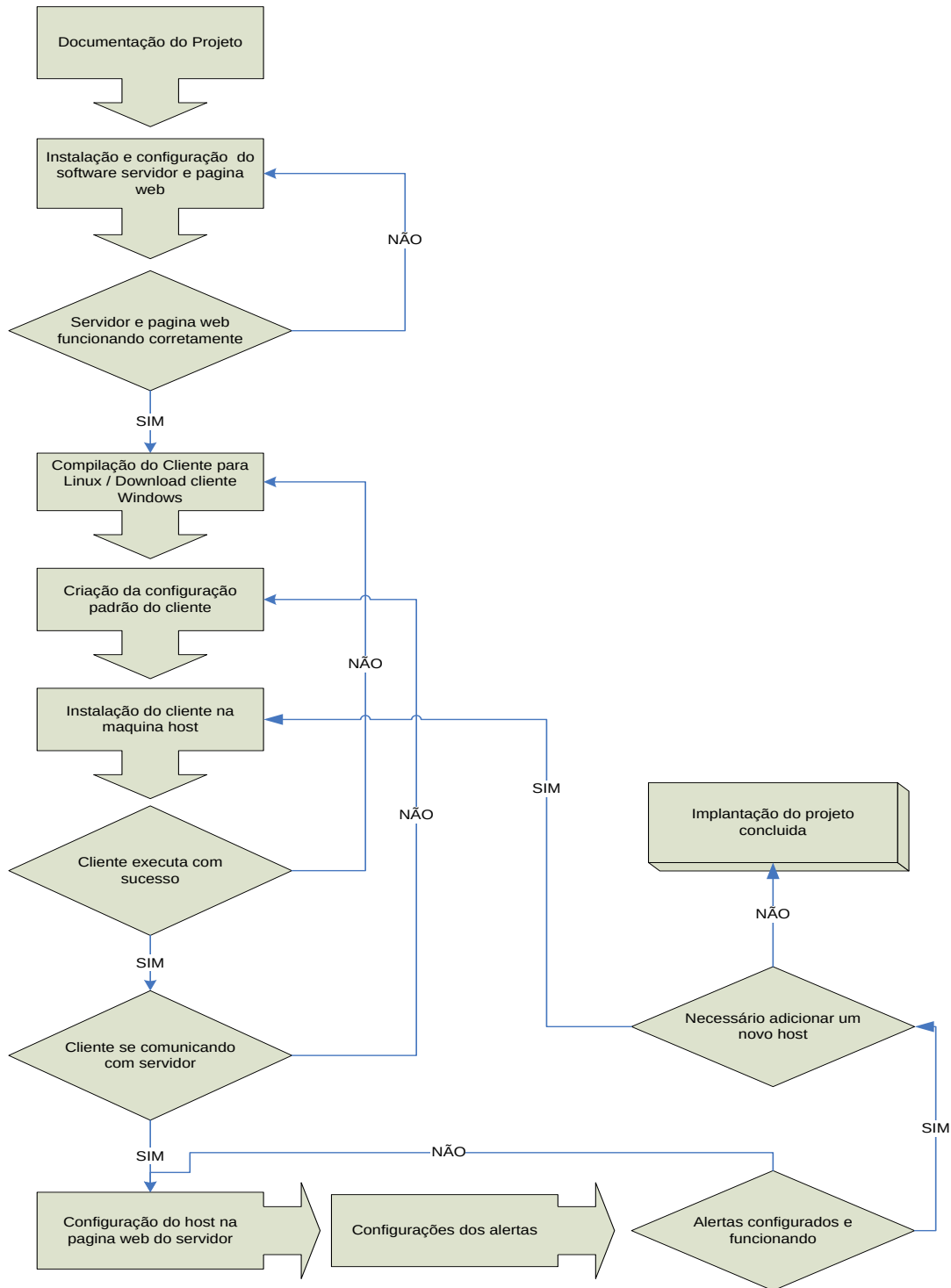
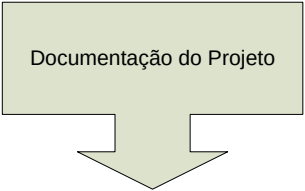
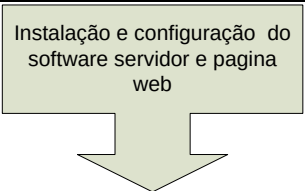
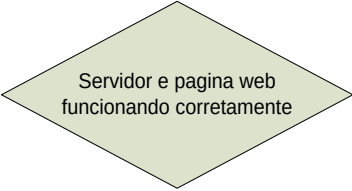
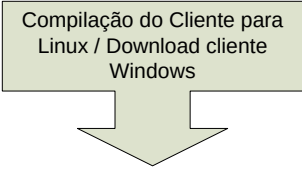
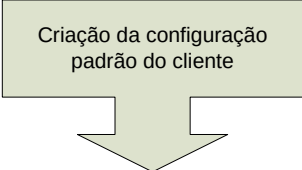


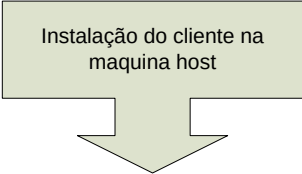
Figura 1

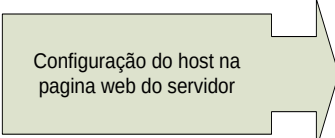
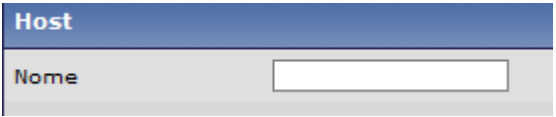
3.2. Descrição do Diagrama de Blocos

Abaixo temos uma tabela descrevendo cada bloco do diagrama.

	Confecção do documento do projeto.
	Executar a compilação/instalação do software no servidor e configuração da página web para acesso dos administradores e usuários. Nesse projeto será utilizado um servidor com o sistema operacional Linux Red Hat AS 4 (http://www.redhat.com/rhel/server/advanced/ , 09/2009), banco de dados Mysql 5 (http://www.mysql.com , 09/2009), servidor web Apache 2 (http://httpd.apache.org/docs/2.0/ , 09/2009) com PHP 5.2 (http://www.php.net , 09/2009), e o Zabbix 1.6.6 (http://zabbix.org/rn1.6.6.php , 09/2009). Hardware é uma maquina com processador de dois núcleos Intel® Xeon™ CPU 3.00GHz, 8GB de RAM e disco SCSI com capacidade de 60GB. A instalação e compilação do Zabbix serão feitas conforme indicado no manual fornecido pelo desenvolvedor no link (http://www.zabbix.com/downloads/ZABBIX%20Manual%20v1.6.pdf , pag. 42, 09/2009). Nos testes executados foi verificado que o ideal é compilar o Zabbix Server, com a opção <i>--enable-static</i> para ser compatível com o maior número de distribuições Linux, pois compila o executável com as bibliotecas necessárias, exceto se o sistema for Solaris que será necessário compilar o cliente num sistema operacional Solaris. Para a instalação da página WEB é necessário copiar a pasta “frontends/php” do diretório de instalação para o diretório padrão de páginas WEB do Apache

	(geralmente /var/www).
	Verificação do servidor e página web, caso todos funcionando corretamente ir para a próxima etapa e se não voltar à etapa anterior. Para checar o funcionamento da página web acessar o endereço HTTP://IP.DO.SERVIDOR/PASTA , será necessário também ter em mãos os dados de acesso ao banco de dados Mysql, se esse foi escolhido na etapa de compilação, após o primeiro acesso a pagina aonde é configurado os dados finais, checar se a página acessa normalmente.
	Executar a compilação do cliente Linux com os códigos fontes do Zabbix e fazer o download cliente Windows. O download do cliente do agente Zabbix para Windows pode ser feito em http://www.suiviperf.com/zabbix/ , aonde está disponível também o manual de instalação e configuração. A compilação do agente Zabbix para Linux é feita a partir do código fonte, cujo qual foi feito o download na etapa de compilação do agente servidor. Dentro da pasta do Zabbix executar o procedimento descrito no manual (http://www.zabbix.com/downloads/ZABBIX%20Manual%20v1.6.pdf , pag. 52, 09/2009), o agente ficará disponível no caminho "src/zabbix_agent/zabbix_agentd" e o arquivo de configuração exemplo ficará disponível no caminho "misc/conf/zabbix_agentd.conf".
	Etapa onde será editado um arquivo de configuração padrão para o agente cliente do Zabbix, que deve ter poucas alterações para se incluir um novo host. Com o arquivo exemplo de configuração disponível no caminho (misc/conf/zabbix_agentd.conf). Serão editados os seguintes parâmetros de configuração:

	#Colocar o IP/HOSTNAME do servidor na linha abaixo #no lugar de 127.0.0.1 <i>Server=127.0.0.1</i> #Descomentar a linha abaixo <i>EnableRemoteCommands=1</i> #Na linha abaixo deverá ser colocado o hostname da #maquina cliente <i>Hostname=Hostname_cliente</i>
	Com o executável do agente Linux ou Windows, enviar ao host e fazer as devidas alterações no arquivo de configuração. Para a instalação na maquina cliente sempre deverá ser criado o usuário zabbix no sistema por questões de segurança, caso contrario o agente do Zabbix será executado com usuário que executou a inicialização do agente. Alterar a linha “<i>Hostaneme=Hostname_cliente</i>” do arquivo <code>zabbix_agentd.conf</code> e copiar para a pasta <code>/etc/zabbix/</code> o binário <code>zabbix_agentd</code> pode ser colocado no caminho <code>/usr/bin/</code>.
	Checar se o cliente executa corretamente, caso positivo ir a próxima etapa caso não, voltar à etapa de compilação do cliente. Para testar o cliente executar ele com a linha abaixo: <code>\$ /usr/bin/zabbix_agentd</code> E verificar se o agente está rodando <code>\$ ps aux grep zabbix_agentd</code>

	O retorno deverá ser mais ou menos assim: <pre>zabbix 5328 0.0 0.0 4512 548 ? SN Sep23 0:00 /usr/bin/zabbix_agentd zabbix 5331 0.1 0.0 4512 848 ? SN Sep23 8:27 /usr/bin/zabbix_agentd</pre>
	Checar no servidor se o cliente está se comunicando com sucesso com o serviço servidor caso positivo ir a próxima etapa caso não voltar para a criação da configuração do cliente. Executar um tail no arquivo de log do cliente para checar se ouve algum erro de configuração do sistema. <pre>\$ tail -f /tmp/zabbix_agentd.log</pre>
	Configurar o host cliente na página servidor como adicionar no grupo e configurar as permissões de acesso. A configuração está disponível conforme exemplificado na Figura 2:  Figura 2 No campo <i>Nome</i> digita o apelido do host:  Figura 3 No campo <i>Grupos</i> adicione o host num grupo ou em vários grupos específicos, isso facilita na administração de permissões de acesso aos hosts.

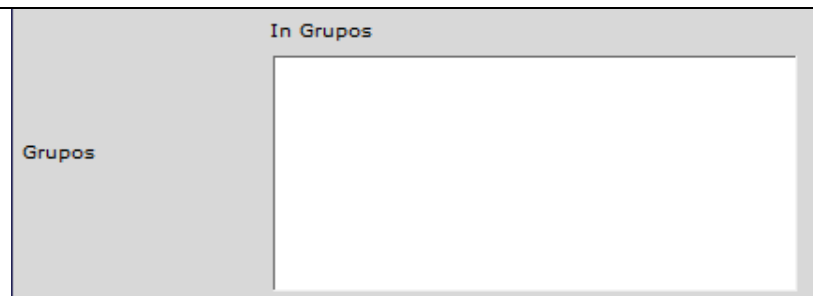


Figura 4

Utilize o campo *Novo Grupo* caso queira criar um novo grupo rapidamente para esse host.



Figura 5

Os campos *Nome DNS* é o hostname completo para acesso do host, o campo *Endereço IP* é o endereço IP do host e o *Conectado a* deve ser marcado como o Zabbix Server acessara a maquina, resolvendo o Nome DNS ou diretamente por IP.

Nome DNS	
Endereço IP	0.0.0.0
Conectado a	Nome DNS ▼

Figura 6

A opção *Associar a Template*, é aonde se vincula o host a um grupo de itens a serem monitorados

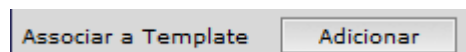
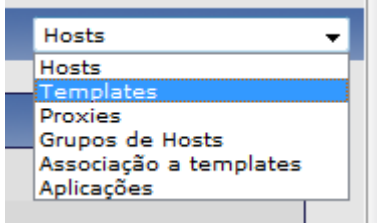
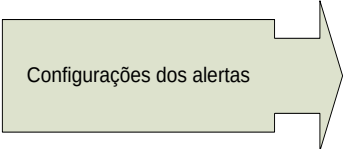
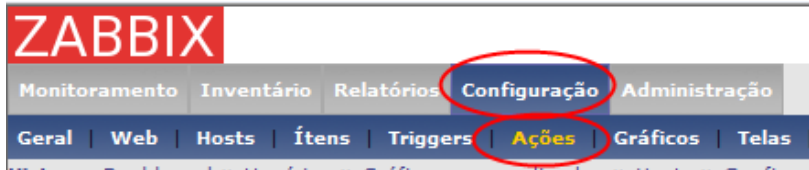
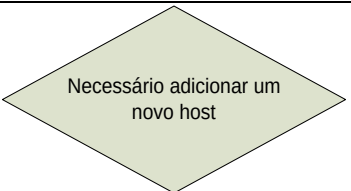


Figura 7

OBS: Os templates podem ser acessados, alterado a opção host por Templates na tela dos Hosts.

	 Hosts Hosts Templates Proxies Grupos de Hosts Associação a templates Aplicações Figura 8
 Configurações dos alertas	Configuração dos itens a serem monitorados e alertas a serem enviados. Os alertas são configurados na aba Ações conforme Figura 9:  Figura 9 Informações mais detalhadas de configuração do alertas podem ser encontrados na pagina 151 no manual do Zabbix.
 Alertas configurados e funcionando	Executar um teste com o sistema de monitoramento e alerta para checar seu correto funcionamento. Forçar uma situação no servidor para simular o envio de e-mail em um caso real.
 Necessário adicionar um novo host	Verificar a necessidade de adicionar um novo host caso sim voltar à etapa de instalação do cliente no host.

Implantação do projeto concluída	Implantação do projeto concluído com sucesso.
----------------------------------	---

4. Procedimentos de Teste e Avaliação

Foi definido um procedimento de testes, aonde foram incluídos 68 hosts (entre servidores Linux/Windows, switch e equipamentos de redes), com *Templates* de monitoração diferentes tendo um total de 3328 itens monitorados.

Foram escolhidos os hosts mais diversificadamente possível, afim de testar todos os componentes de software.

ZABBIX		Help Suporte Print Configurações Logout
Monitoramento	Inventário	Relatórios
Status do ZABBIX Relatório de disponibilidade Triggers mais ativadas - top 100		
History: Dados recentes » Dados recentes » Status do ZABBIX » Dashboard » Dados do host		
STATUS DO ZABBIX		
Parâmetro	Valor	Detalhes
ZABBIX está rodando	Sim	-
Número de hosts (monitored/not monitored/templates/removido)	131	68 / 6 / 57
Número de itens (monitorados/desativados/não suportado)[trapper]	7040	3328 / 2779 / 933
Número de triggers (ativas/desativadas)[verdadeiro/desconhecido/falso]	1115	1103 / 12 [9 / 47 / 1047]
Número de usuários (online)	9	2
Required server performance, new values per second	23.23	-
Atualizado: 14:01:27		
ZABBIX 1.6.6 Copyright 2001-2009 by		
Conectado como 'rceluppi'		

Figura 10

Os *Templates* foram alterados para capturar os dados do sistema a cada 300 segundos (5 minutos), visto que por padrão a maioria dos dados é capturado a cada 30 segundos gerando uma carga excessiva no servidor Zabbix e no banco de dados Mysql.

Na Figura 11 com os dados dos últimos 7 dias podemos ver que com o numero de hosts atuais o Zabbix gera uma quantidade de em média 165 queries SQL por segundo:

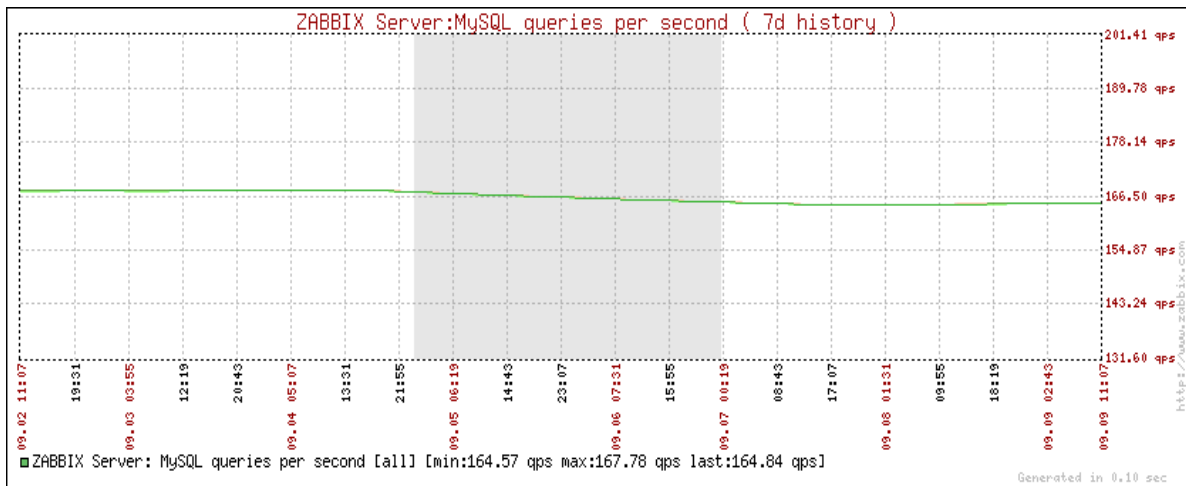


Figura 11

Gerando um load 15 na maquina de em média 1, conforme demonstra a Figura 12:

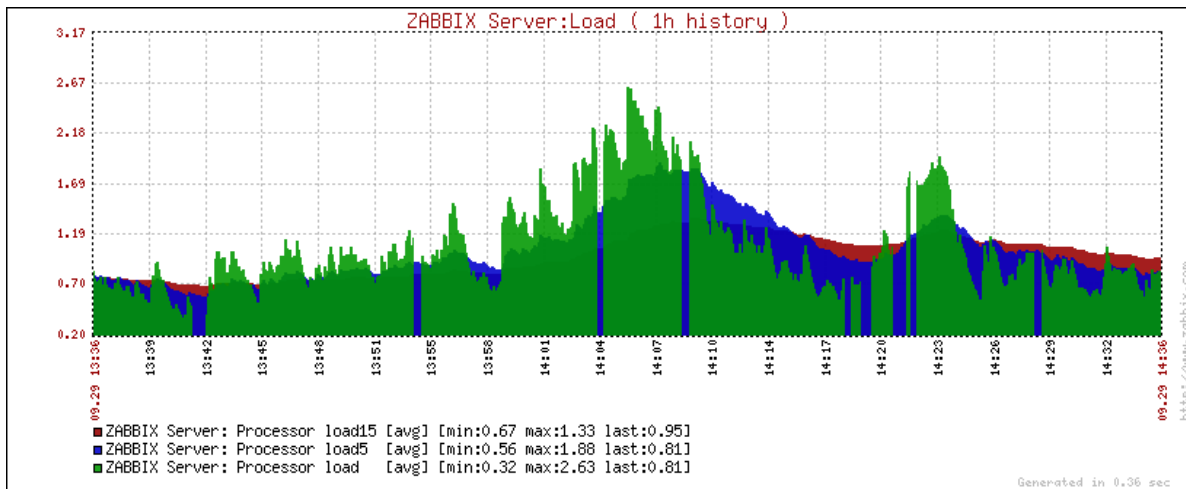


Figura 12

Foi monitorada também a utilização de memória [Figura 13], rede [Figura 14] e disco [Figura 15]:

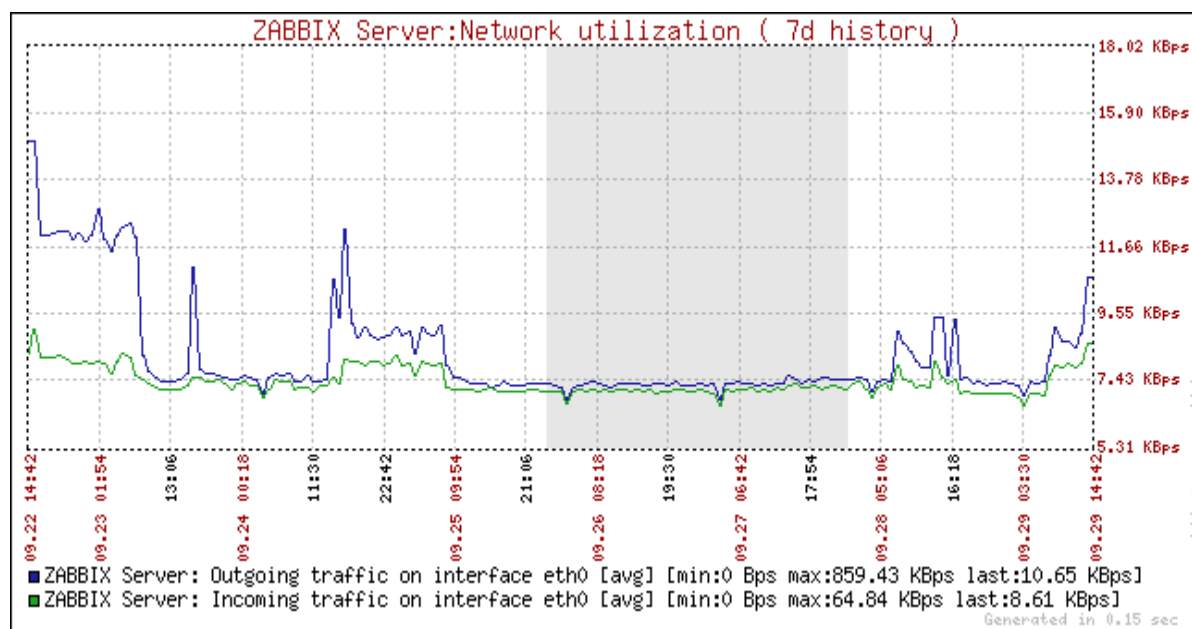


Figura 13

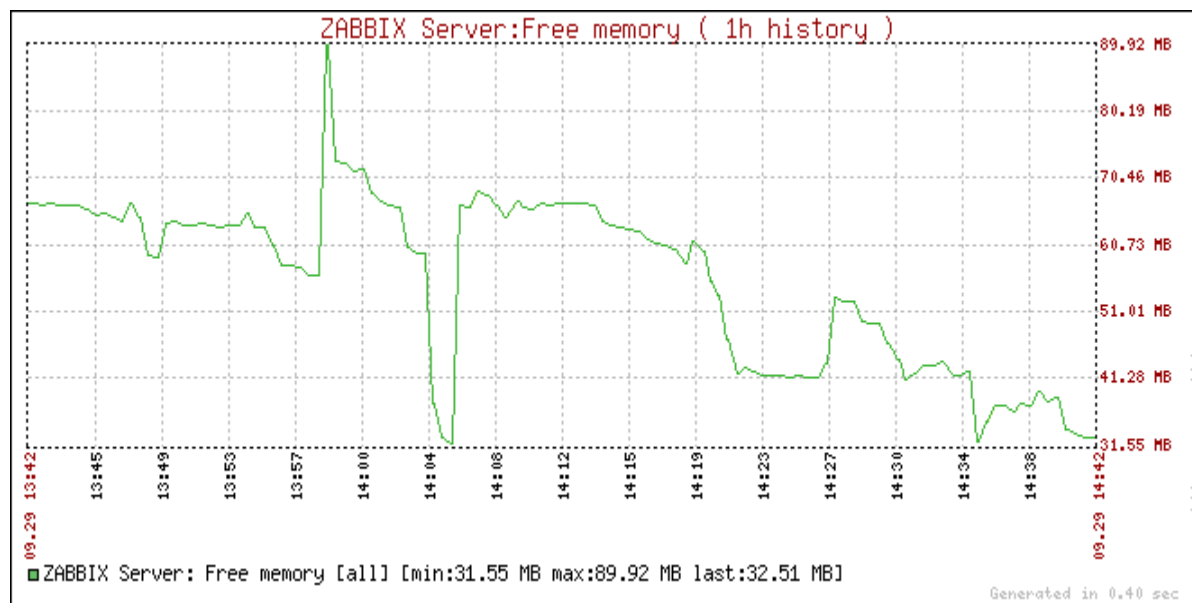


Figura 14

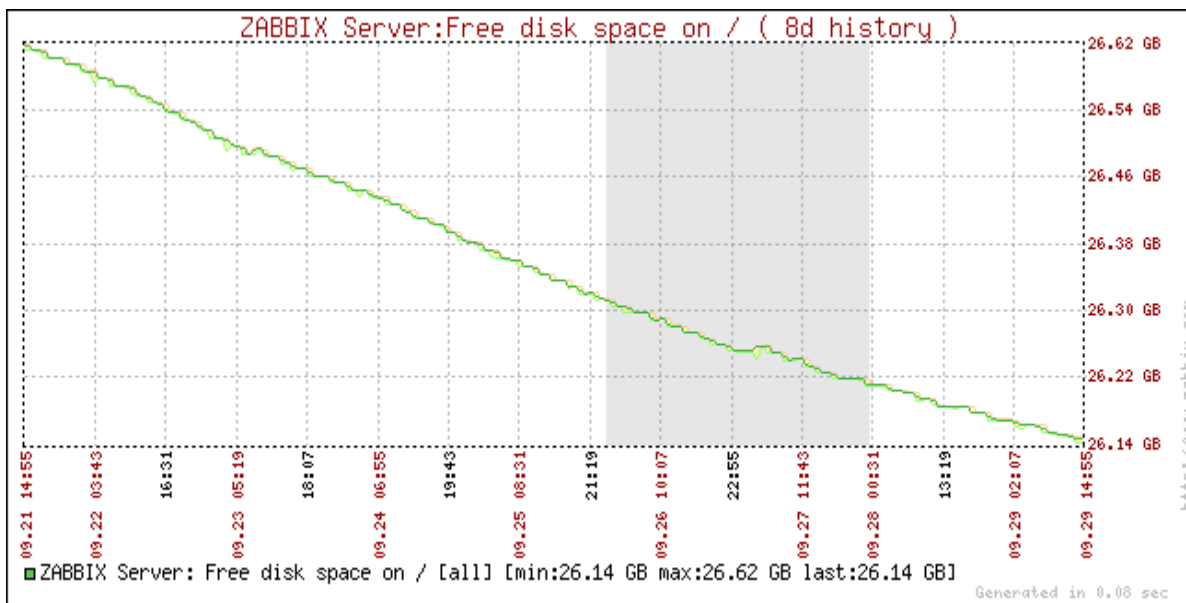


Figura 15

Concluimos com os gráficos [Figura 13],[Figura 14] e [Figura 15] que será necessária a utilização de uma maquina com processador de quatro núcleos para atingirmos os 120 hosts necessários com folga de processamento para futura ampliação dos hosts e o restante do hardware é o suficiente para atender as necessidades.

Os testes de funcionalidades de software também foram executados com sucesso, aonde os alertas configurados foram enviados com sucesso ao grupo de usuários configurado, segue abaixo um exemplo do e-mail enviado:

```
-----Mensagem original-----
De: zabbix@xxxxxxpr.com.br [mailto:zabbix@xxxxxxpr.com.br] Enviada em: terça-feira, 29 de setembro de 2009 14:31
Para: FDPR-INFO-Carlos Alxxxxx Hxxxxxx
Assunto: uni975dw: Processor load is too high on uni975dw: OK

Processor load is too high on uni975dw: OK

Ultimo valor:
9.23
```

A Figura 16 demonstra o relatório dos últimos 20 incidentes gerados e ao lado o numero de ações gerada.

Last 20 issues					
Host	Issue	Última alteração	Age	Visto	Ações
s975lmig01	Version of zabbix_agent(d) was changed on s975lmig01	29 Sep 15:12:47	47s	Não	2
s975lhilum	Processor load is too high on s975lhilum	29 Sep 15:07:59	5m 35s	Não	-
uni168sby	Erro Sincronismo Oracle Standby	29 Sep 14:53:56	19m 38s	Não	2
tomcat_s975lhilumsby_unimedpr_com_br	tomcat_s975lhilumsby_unimedpr_com_br uses suboptimal jit compiler	29 Sep 04:35:39	10h 37m 55s	Não	-
uni151sby	Server uni151sby is unreachable	21 Sep 16:48:20	1w 22h	Não	2
s975wsq102	Low free disk space on s975wsq102 volume d:	18 Sep 01:13:56	1w 4d 13h	Não	2
s076lfw01	Server s076lfw01 is unreachable	16 Sep 17:20:01	1w 5d 21h	Não	-
s975wdom01	Low free disk space on s975wdom01 volume g:	13 Sep 03:09:49	2w 2d 12h	Não	-
s975wdom01	Low free disk space on s975wdom01 volume f:	13 Sep 03:09:47	2w 2d 12h	Não	-
Atualizado: 15:13:34					

Figura 16

Também foi possível monitorar nossos sistemas web, com a utilização da funcionalidade do Zabbix que permite monitorar cenários web, a Figura 17 demonstra um exemplo de relatório de cenário web.

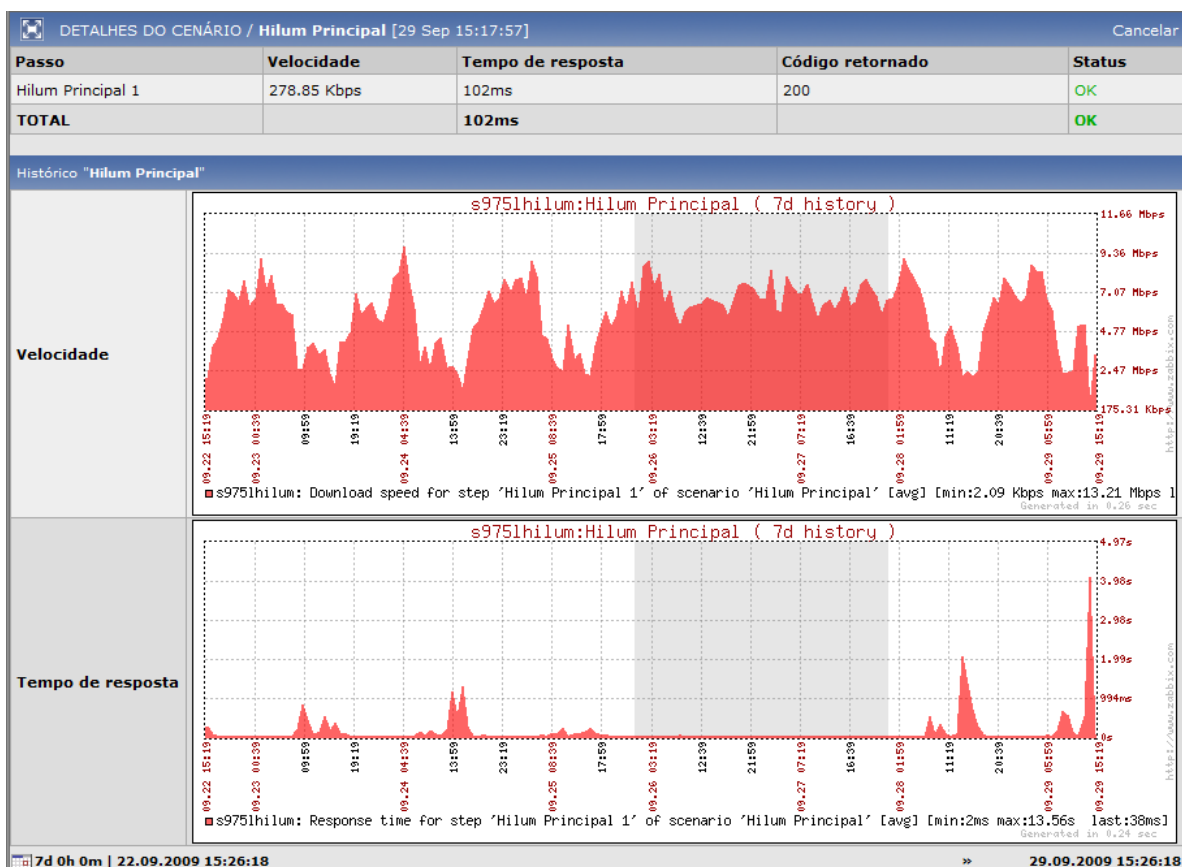
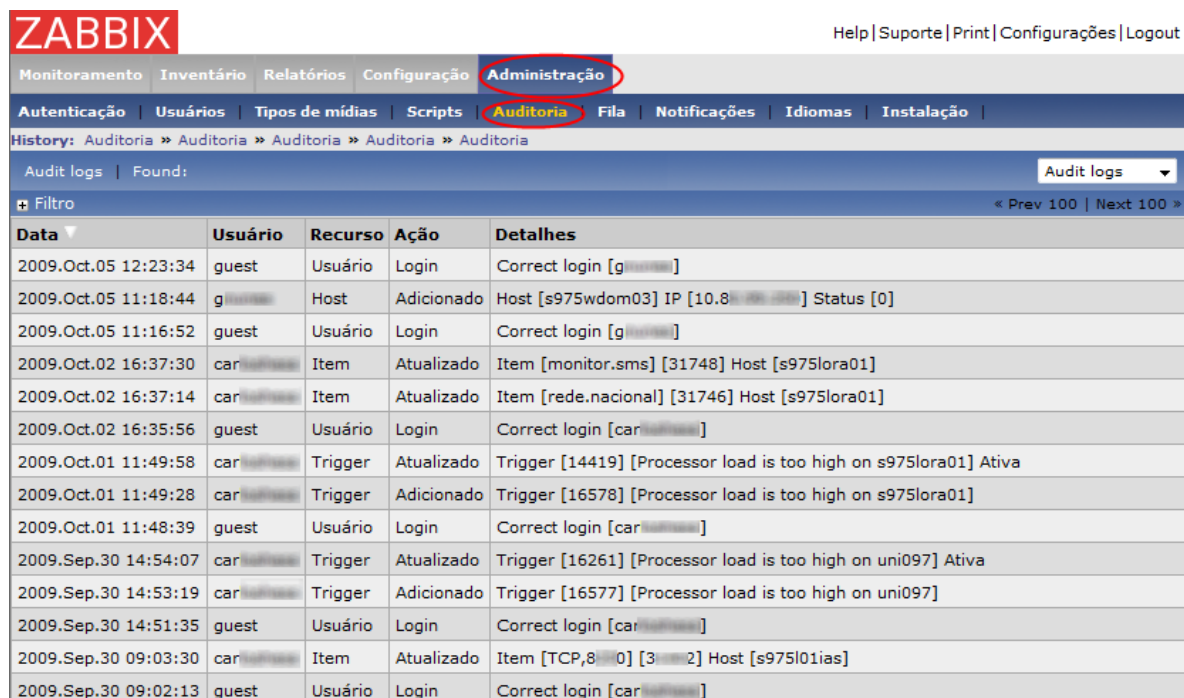


Figura 17

Na Figura 18 podemos ver o relatório de auditoria que o Zabbix disponibiliza para garantir a integridade das informações:



Data	Usuário	Recurso	Ação	Detalhes
2009.Oct.05 12:23:34	guest	Usuário	Login	Correct login [g...]
2009.Oct.05 11:18:44	g...	Host	Adicionado	Host [s975wdom03] IP [10.8...] Status [0]
2009.Oct.05 11:16:52	guest	Usuário	Login	Correct login [g...]
2009.Oct.02 16:37:30	car...	Item	Atualizado	Item [monitor.sms] [31748] Host [s975lora01]
2009.Oct.02 16:37:14	car...	Item	Atualizado	Item [rede.nacional] [31746] Host [s975lora01]
2009.Oct.02 16:35:56	guest	Usuário	Login	Correct login [car...]
2009.Oct.01 11:49:58	car...	Trigger	Atualizado	Trigger [14419] [Processor load is too high on s975lora01] Ativa
2009.Oct.01 11:49:28	car...	Trigger	Adicionado	Trigger [16578] [Processor load is too high on s975lora01]
2009.Oct.01 11:48:39	guest	Usuário	Login	Correct login [car...]
2009.Sep.30 14:54:07	car...	Trigger	Atualizado	Trigger [16261] [Processor load is too high on uni097] Ativa
2009.Sep.30 14:53:19	car...	Trigger	Adicionado	Trigger [16577] [Processor load is too high on uni097]
2009.Sep.30 14:51:35	guest	Usuário	Login	Correct login [car...]
2009.Sep.30 09:03:30	car...	Item	Atualizado	Item [TCP,8...0] [3...2] Host [s975l01ias]
2009.Sep.30 09:02:13	guest	Usuário	Login	Correct login [car...]

Figura 18

5. Conclusão

Como resultado de todos os estudos realizados nesse projeto, concluímos que o Zabbix atende a todos os requisitos do projeto e agrega mais valor a infraestrutura atual da nossa empresa, nos auxilia no cumprimento de todos os nossos contratos SLA's, cria relatórios gerenciais confiáveis, entre outras funções.

O único ponto mais negativo encontrado foi que o Zabbix é desenvolvido por uma empresa privada com fins lucrativos, podendo descontinuar o desenvolvimento do produto a qualquer momento, além do suporte também ser pago caso necessário, mas por ser open source acredita-se que o desenvolvimento se continuara pela comunidade open source.

Com a implantação do Zabbix em nossa infraestrutura, teremos melhores condições de agir de maneira pró ativa nos problemas que possam acontecer de rede, assim como manter um histórico de toda nossa infraestrutura afim de diagnósticos posteriores tanto como para fins de auditoria . Monitorando rapidamente nossos contratos de SLA assim garantindo um atendimento eficiente e a satisfação dos nossos clientes.

Fica indicado à implantação da funcionalidade do Zabbix abrir incidentes diretamente no software de controle de incidentes utilizado pela empresa RITM via script, indicamos também em caso de ampliação dos números de hosts monitorados a separação do banco de dados do agente servidor do Zabbix.

Índices de Figuras

Figura 1	8
Figura 2	12
Figura 3	12
Figura 4	13
Figura 5	13
Figura 6	13
Figura 7	13
Figura 8	14
Figura 9	14
Figura 10	15
Figura 11	16
Figura 12	16
Figura 13	17
Figura 14	17
Figura 15	18
Figura 16	19
Figura 17	19
Figura 18	20

Referencias Bibliográficas

- [1] <http://www.zabbix.com> (09/2009)
- [2] <http://www.nagios.org> (09/2009)
- [3] <http://www.cacti.net> (09/2009)
- [4] <http://www.zabbix.com/downloads/ZABBIX%20Manual%20v1.6.pdf> (09/2009)